HIDDEN IDENTIFICATION

Inventors:

Ronald P. Cocchi
Christopher P. Curren
Raynold M. Kahn

HIDDEN IDENTIFICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

5   [0001]   This application is related to the following co-pending and commonly-assigned patent

applications, which applications are incorporated by reference herein:

[0002]   United States Patent Application Serial No. xx/xxx,xxx, entitled "MULTIPLE

NONVOLATILE MEMORIES", by Ronald Cocchi, et. al., Attorney Docket No. PD-

200335, filed on the same date herewith;

10   [0003]   United States Patent Application Serial No. xx/xxx,xxx, entitled "DEDICATED

NONVOLATILE MEMORY", by Ronald Cocchi, et. al., Attorney Docket No. PD-200337,

filed on the same date herewith; and

[0004]   United States Patent Application Serial No. xx/xxx,xxx, entitled

"ASYNCHRONOUS CONFIGURATION", by Ronald Cocchi, et. al., Attorney Docket No.

15   PD-201161, filed on the same date herewith.

BACKGROUND OF THE INVENTION

1.   Field of the Invention

[0005]   The present invention relates to systems and methods for preventing/limiting

20   unauthorized access to digital services and in particular to a method and system for uniquely

identifying nonvolatile memory such that the identity of the memory is hidden.

2.   Description of the Related Art

[0006]   Digital services such as television programs and information regarding those programs

25   (e.g., a program guide) are distributed to users by a variety of broadcasting methods. Such

services may be proprietary and available on a subscription basis. To prevent unauthorized

access to the services, a plethora of security mechanisms are utilized. Such mechanisms may

store information in memory, wherein the information is used to validate a user or provide

access. However, persons often attempt to obtain illegal/unauthorized access to the services by altering or accessing the memory contents. What is needed is the capability to prevent or increase the difficulty of obtaining illegal access to the information and digital services. These problems may be better understood by a description of current broadcasting methods, security

5   mechanisms, and methods for obtaining unauthorized access to such services.

[0007]   As described above, television programs and digital services are distributed to viewers by a variety of broadcasting methods. These methods include traditional analog broadcast television (National Television Systems Committee or "NTSC" standard), the soon to be required digital broadcast television (Advanced Television Systems Committee or "ATSC"

10   standard), cable television (both analog and digital), satellite broadcasting (both analog and digital), as well as other methods. These methods allow channels of television content to be multiplexed and transmitted over a common transmission medium.

[0008]   To view the television programming and have access to the digital services, users commonly have a set top box (also referred to as an integrated receiver/decoder [IRD]).

15   Within the system or set top box, a security component/microcircuit known as a smart card may be utilized to prevent unauthorized access to the television programs and digital services. The smart card microcircuit may contain a microprocessor, volatile memory components, a nonvolatile memory component, and a system input/output module.

[0009]   Nonvolatile memory has been used extensively throughout the electronics industry.

20   For example, in the IRD, the microprocessor utilizes nonvolatile memory to contain state information (e.g., status information) used to provide the desired functionality and enforce security policies intended by the designers. The microprocessor and/or a memory access control unit utilized by the microprocessor restricts access to the memory components.

[0010]   However, there have been numerous attempts by individuals or companies (i.e.,

25   hackers or attackers) to attack, misuse, or modify the nonvolatile memory through external means of reprogramming or otherwise altering the contents of the memory when the memory component has been available to the central processor or otherwise on the system bus. For example, attacks using unforeseen methods or subverting poorly implemented defenses can be

used to gain unauthorized access to the contents of the memory and/or lead to reprogramming the contents of the memory. Reprogramming or unauthorized access to the memory contents can lead to complete compromise of the security features intended in the device.

[0011]   The simplest and most prevalent form of attack against the memory components uses external noninvasive means using a system's input/output module due to the low cost of the equipment required to implement this form of attack. Most attacks occur by inappropriate manipulation of a microprocessor or memory access control unit. For example, memory contents have been subverted when a memory access control unit (that controls access to a memory component) has been compromised. Once the single memory component has been breached, the attacker may then have the capability to access all memory address locations that reside in other memory components.

[0012]   An example of unauthorized access to digital services occurs when a smart card or memory component is cloned. In such a low cost cloning attack, the identity of a pirate card is copied to a new card. Accordingly, smart cards/memory components have an identity/identification number. In the prior art, the identification number may be established as a hardwired identification number in read only memory (ROM). However, using a new ROM mask with a hardwired identification number for each chip produced is expensive and time consuming. Further, identification numbers in the prior art are accessible to the system input/output module, system bus, microprocessor, or external environment, thereby allowing attacks to the system.

SUMMARY OF THE INVENTION

[0013]   Digital services systems often contain a service module known as a smart card to prevent unauthorized access to the services. The smart card microcircuit contains a microprocessor, volatile memory components, nonvolatile memory components, a custom logic block, and a system input/output module. The security system may be compromised if memory components are used or attacked in unattended ways.

[0014]   One or more embodiments of the invention provide a method, apparatus, and article of manufacture for incorporating a hidden identification number into some form of nonvolatile memory. The identification number is hidden from the microprocessor by placing the number in a memory location that is not accessible by the system input/output module, system bus,
5   microprocessor, or external environment. The nonvolatile memory is read only through a custom logic block. The identification number is protected because it is not accessible by the microprocessor and hence cannot be altered by external means. Further, the identification number uniquely identifies the device that contains the nonvolatile memory and is associated with and used to determine access rights/privileges to digital services.

10

BRIEF DESCRIPTION OF THE DRAWINGS

[0015]   Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

[0016]   FIG. 1 is a diagram showing an overview of a video distribution system;

15   [0017]   FIG. 2 is a block diagram showing a typical uplink configuration showing how video program material is uplinked to a satellite for transmission to subscribers using a single transponder;

[0018]   FIG. 3 is a block diagram of one embodiment of the program guide subsystem;

[0019]   FIG. 4A is a diagram of a representative data stream received from a satellite;

20   [0020]   FIG. 4B is a diagram illustrating the structure of a data packet;

[0021]   FIG. 5 is a block diagram of one embodiment of an integrated receiver/decoder;

[0022]   FIGS. 6A and 6B illustrate architectures of a conditional access module in accordance with one or more embodiments of the invention; and

[0023]   FIG. 7 is a flow chart illustrating the use of a hidden identification number to limit
25   unauthorized access to digital services in accordance with one or more embodiments of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0024]   In the following description reference is made to the accompanying drawings which form a part hereof and which show, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Overview

[0025]   A non-modifiable protected/hidden identification number is embedded into a nonvolatile memory component. The hidden identification number is not accessible through a system input/output module, system bus, microprocessor, or external environment. The hidden identification is programmed after manufacturing and makes the nonvolatile memory component (and thereby the chip containing the memory component) unique.

Video Distribution System

[0026]   FIG. 1 is a diagram illustrating an overview of a single satellite video distribution system 100. The video distribution system 100 comprises a control center 102 in communication with an uplink center 104 via a ground or other link 114 and with a subscriber receiver station 110 via a public switched telephone network (PSTN) or other link 120. The control center 102 provides program material (e.g. digital services, video programs, audio programs and data) to the uplink center 104 and coordinates with the subscriber receiver stations 110 to offer, for example, pay-per-view (PPV) program services, including billing and associated decryption of video programs.

[0027]   The uplink center 104 receives program material and program control information from the control center 102, and using an uplink antenna 106 and transmitter 105, transmits the program material and program control information to the satellite 108 via uplink 116. The satellite receives and processes this information, and transmits the video programs and control information to the subscriber receiver station 110 via downlink 118 using transmitter 107. The

subscriber receiving station 110 receives this information using the outdoor unit (ODU) 112, which includes a subscriber antenna and a low noise block converter (LNB).

[0028] The subscriber receiving station 110 permits the use/viewing of the information by a subscriber 122. For example, the information may be used/viewed on a television 124 or other display device. To control access to the information, the subscriber receiving station 110 includes an integrated receiver/decoder (IRD) 126. In embodiments of the invention, the IRD 126 is communicatively coupled to a security component known as a conditional access module or smart card that controls access to the information/digital services.

[0029] In one embodiment, the subscriber receiving station antenna is an 18-inch slightly oval-shaped Ku-band antenna. The slight oval shape is due to the 22.5 degree offset feed of the LNB (low noise block converter) which is used to receive signals reflected from the subscriber antenna. The offset feed positions the LNB out of the way so it does not block any surface area of the antenna minimizing attenuation of the incoming microwave signal.

[0030] The video distribution system 100 can comprise a plurality of satellites 108 in order to provide wider terrestrial coverage, to provide additional channels, or to provide additional bandwidth per channel. In one embodiment of the invention, each satellite comprises 16 transponders to receive and transmit program material and other control data from the uplink center 104 and provide it to the subscriber receiving stations 110. Using data compression and multiplexing techniques the channel capabilities, two satellites 108 working together can receive and broadcast over 150 conventional (non-HDTV) audio and video channels via 32 transponders.

[0031] While the invention disclosed herein will be described with reference to a satellite-based video distribution system 100, the present invention may also be practiced with terrestrial-based transmission of program information, whether by broadcasting means, cable, or other means. Further, the different functions collectively allocated among the control center 102 and the uplink center 104 as described above can be reallocated as desired without departing from the intended scope of the present invention.

[0032]   Although the foregoing has been described with respect to an embodiment in which the program material delivered to the subscriber 122 is video (and audio) program material such as a movie, the foregoing method can be used to deliver program material comprising purely audio information or other data as well.

5

Uplink Configuration

[0033]   FIG. 2 is a block diagram showing a typical uplink configuration for a single satellite 108 transponder, showing how video program material is uplinked to the satellite 108 by the control center 102 and the uplink center 104. FIG. 2 shows three video channels (which could

10   be augmented respectively with one or more audio channels for high fidelity music, soundtrack information, or a secondary audio program for transmitting foreign languages), a data channel from a program guide subsystem 206 and computer data information from a computer data source 208.

[0034]   The video channels are provided by a program source of video material 200A-200C

15   (collectively referred to hereinafter as video source(s) 200). The data from each video program source 200 is provided to an encoder 202A-202C (collectively referred to hereinafter as encoder(s) 202). Each of the encoders accepts a program time stamp (PTS) from the controller 216. The PTS is a wrap-around binary time stamp that is used to assure that the video information is properly synchronized with the audio information after encoding and

20   decoding. A PTS time stamp is sent with each I-frame of the MPEG encoded data.

[0035]   In one embodiment of the present invention, each encoder 202 is a second generation Motion Picture Experts Group (MPEG-2) encoder, but other decoders implementing other coding techniques can be used as well. The data channel can be subjected to a similar compression scheme by an encoder (not shown), but such compression is usually either

25   unnecessary, or performed by computer programs in the computer data source (for example, photographic data is typically compressed into *.TIF files or *.JPG files before transmission). After encoding by the encoders 202, the signals are converted into data packets by a packetizer

204A-204F (collectively referred to hereinafter as packetizer(s) 204) associated with each source 200.

[0036]   The data packets are assembled using a reference from the system clock 214 (SCR), and from the conditional access manager 210, which provides the SCID to the packetizers 204 for use in generating the data packets. These data packets are then multiplexed into serial data and transmitted.

Program Guide Subsystem

[0037]   FIG. 3 is a block diagram of one embodiment of the program guide subsystem 206. The program guide data transmitting system 206 includes program guide database 302, compiler 304, sub-databases 306A-306C (collectively referred to as sub-databases 306) and cyclers 308A- 308C (collectively referred to as cyclers 308).

[0038]   Schedule feeds 310 provide electronic schedule information about the timing and content of various television channels, such as that found in television schedules contained in newspapers and television guides. Schedule feeds 310 preferably include information from one or more companies that specialize in providing schedule information, such as TRIBUNE MEDIA SERVICES™, and T.V. DATA™. The data provided by companies such as TRIBUNE MEDIA SERVICES™ and T.V. DATA™ are typically transmitted over telephone lines to program guide database 302. These companies provide television schedule data for all of the television stations across the nation plus the nationwide channels, such as SHOWTIME™, HBO™, and the DISNEY CHANNEL™. The specific format of the data that are provided by these companies varies from company to company. Program guide database 302 preferably includes schedule data for television channels across the entire nation including all nationwide channels and local channels, regardless of whether the channels are transmitted by the transmission station.

[0039]   Program guide database 302 is a computer-based system that receives data from schedule feeds 310 and organizes the data into a standard format. Compiler 304 reads the standard form data out of program guide database 302, identifies common schedule portions,

converts the program guide data into the proper format for transmission to users (specifically, the program guide data are converted into objects as discussed below) and outputs the program guide data to one or more of sub-databases 306.

[0040]   Program guide data can also be manually entered into program guide database 302 through data entry station 312. Data entry station 312 allows an operator to enter additional scheduling information, as well as combining and organizing data supplied by the scheduling companies. As with the computer organized data, the manually entered data are converted by the compiler into separate objects and sent to one or more of sub-databases 306.

[0041]   The program guide objects are temporarily stored in sub-databases 306 until cyclers 308 request the information. Each of cyclers 308 may transmit objects at a different rate than the other cyclers 308. For example, cycler 308A may transmit objects every second, while cyclers 308B and 308C may transmit objects every 5 seconds and every 10 seconds, respectively.

[0042]   Since the subscriber's receivers may not always be on and receiving and saving objects, the program guide information is continuously re-transmitted. Program guide objects for programs that will be shown in the next couple of hours are sent more frequently than program guide objects for programs that will be shown later. Thus, the program guide objects for the most current programs are sent to a cycler 308 with a high rate of transmission, while program guide objects for later programs are sent to cyclers 308 with a lower rate of transmission. One or more of the data outputs 314 of the cyclers 308 are forwarded to the packetizer of a particular transponder, as depicted in FIG. 2.

[0043]   It is noted that the uplink configuration depicted in FIG. 2 and the program guide subsystem depicted in FIG. 3 can be implemented by one or more hardware modules, one or more software modules defining instructions performed by a processor, or a combination of both.

Broadcast Data Stream Format and Protocol

[0044]   FIG. 4A is a diagram of a representative data stream. The first packet segment 402 comprises information from video channel 1 (data coming from, for example, the first video program source 200A). The next packet segment 404 comprises computer data information

5   that was obtained, for example from the computer data source 208. The next packet segment 406 comprises information from video channel 5 (from one of the video program sources 200). The next packet segment 408 comprises program guide information such as the information provided by the program guide subsystem 206. As shown in FIG. 4A, null packets 410 created by the null packet module 212 may be inserted into the data stream as desired.

10   [0045]   The data stream therefore comprises a series of packets from any one of the data sources in an order determined by the controller 216. The data stream is encrypted by the encryption module 218, modulated by the modulator 220 (typically using a QPSK modulation scheme), and provided to the transmitter 222, which broadcasts the modulated data stream on a frequency bandwidth to the satellite via the antenna 106. The receiver 126 receives these

15   signals, and using the SCID, reassembles the packets to regenerate the program material for each of the channels.

[0046]   FIG. 4B is a diagram of a data packet. Each data packet (e.g. 402-416) is 147 bytes long, and comprises a number of packet segments. The first packet segment 420 comprises two bytes of information containing the SCID and flags. The SCID is a unique 12-bit number

20   that uniquely identifies the data packet's data channel. The flags include 4 bits that are used to control other features. The second packet segment 422 is made up of a 4-bit packet type indicator and a 4 -bit continuity counter. The packet type identifies the packet as one of the four data types (video, audio, data, or null). When combined with the SCID, the packet type determines how the data packet will be used. The continuity counter increments once for each

25   packet type and SCID. The next packet segment 424 comprises 127 bytes of payload data, which in the cases of packets 402 or 406 is a portion of the video program provided by the video program source 200. The final packet segment 426 is data required to perform forward error correction.

Integrated Receiver/Decoder

[0047]   FIG. 5 is a block diagram of an integrated receiver/decoder (IRD) 126 (also
hereinafter alternatively referred to as receiver 126 or a set top box). The receiver 126
5   comprises a tuner/demodulator 504 communicatively coupled to an ODU 112 having one or
more LNBs 502. The LNB 502 converts the 12.2- to 12.7 GHz downlink 118 signal from the
satellites 108 to, e.g., a 950-1450 MHz signal required by the IRD's 126 tuner/demodulator
504. The LNB 502 may provide either a dual or a single output. The single-output LNB 502
has only one RF connector, while the dual output LNB 502 has two RF output connectors and
10   can be used to feed a second tuner 504, a second receiver 126, or some other form of
distribution system.

[0048]   The tuner/demodulator 504 isolates a single, digitally modulated 24 MHz transponder,
and converts the modulated data to a digital data stream. The digital data stream is then
supplied to a forward error correction (FEC) decoder 506. This allows the IRD 126 to
15   reassemble the data transmitted by the uplink center 104 (which applied the forward error
correction to the desired signal before transmission to the subscriber receiving station 110)
verifying that the correct data signal was received, and correcting errors, if any. The error-
corrected data may be fed from the FEC decoder module 506 to the transport module 508 via
an 8-bit parallel interface.

20   [0049]   The transport module 508 performs many of the data processing functions performed
by the IRD 126. The transport module 508 processes data received from the FEC decoder
module 506 and provides the processed data to the video MPEG decoder 514 and the audio
MPEG decoder 517. In one embodiment of the present invention, the transport module, video
MPEG decoder and audio MPEG decoder are all implemented on integrated circuits. This
25   design promotes both space and power efficiency, and increases the security of the functions
performed within the transport module 508. The transport module 508 also provides a passage
for communications between the microcontroller 510 and the video and audio MPEG decoders
514, 517. As set forth more fully hereinafter, the transport module also works with the

conditional access module (CAM) 512 to determine whether the subscriber receiving station 110 is permitted to access certain program material. Data from the transport module can also be supplied to external communication module 526.

[0050]   The CAM 512 functions in association with other elements to decode an encrypted

5   signal from the transport module 508. The CAM 512 may also be used for tracking and billing these services. In one embodiment of the present invention, the CAM 512 is a smart card, having contacts cooperatively interacting with contacts in the IRD 126 to pass information. In order to implement the processing performed in the CAM 512, the IRD 126, and specifically the transport module 508 provides a clock signal to the CAM 512. Details of the CAM 512

10   architecture are described below.

[0051]   Video data is processed by the MPEG video decoder 514. Using the video random access memory (RAM) 536, the MPEG video decoder 514 decodes the compressed video data and sends it to an encoder or video processor 516, which converts the digital video information received from the video MPEG module 514 into an output signal usable by a display

15   or other output device. By way of example, processor 516 may comprise a National TV Standards Committee (NTSC) or Advanced Television Systems Committee (ATSC) encoder. In one embodiment of the invention both S-Video and ordinary video (NTSC or ATSC) signals are provided. Other outputs may also be utilized, and are advantageous if high definition programming is processed.

20   [0052]   Audio data is likewise decoded by the MPEG audio decoder 517. The decoded audio data may then be sent to a digital to analog (D/A) converter 518. In one embodiment of the present invention, the D/A converter 518 is a dual D/A converter, one for the right and left channels. If desired, additional channels can be added for use in surround sound processing or secondary audio programs (SAPs). In one embodiment of the invention, the dual D/A

25   converter 518 itself separates the left and right channel information, as well as any additional channel information. Other audio formats may similarly be supported. For example, other audio formats such as multi-channel DOLBY DIGITAL AC-3 may be supported.

[0053]   A description of the processes performed in the encoding and decoding of video streams, particularly with respect to MPEG and JPEG encoding/decoding, can be found in Chapter 8 of "Digital Television Fundamentals," by Michael Robin and Michel Poulin, McGraw-Hill, 1998, which is hereby incorporated by reference herein.

5   [0054]   The microcontroller 510 receives and processes command signals from the remote control 524, an IRD 126 keyboard interface, and/or another input device. The microcontroller receives commands for performing its operations from a processor programming memory, which permanently stores such instructions for performing such commands. The processor programming memory may comprise a read only memory (ROM) 538, an electrically erasable

10   programmable read only memory (EEPROM) 522 or, similar memory device. The microcontroller 510 also controls the other digital devices of the IRD 126 via address and data lines (denoted "A" and "D" respectively, in FIG. 5).

[0055]   The modem 540 connects to the customer's phone line via the PSTN port 120. It calls, e.g. the program provider, and transmits the customer's purchase information for billing

15   purposes, and/or other information. The modem 540 is controlled by the microprocessor 510. The modem 540 can output data to other I/O port types including standard parallel and serial computer I/O ports.

[0056]   The present invention also comprises a local storage unit such as the video storage device 532 for storing video and/or audio data obtained from the transport module 508. Video

20   storage device 532 can be a hard disk drive, a read/writeable compact disc of DVD, a solid state RAM, or any other storage medium. In one embodiment of the present invention, the video storage device 532 is a hard disk drive with specialized parallel read/write capability so that data may be read from the video storage device 532 and written to the device 532 at the same time. To accomplish this feat, additional buffer memory accessible by the video storage

25   532 or its controller may be used. Optionally, a video storage processor 530 can be used to manage the storage and retrieval of the video data from the video storage device 532. The video storage processor 530 may also comprise memory for buffering data passing into and out of the video storage device 532. Alternatively or in combination with the foregoing, a plurality

of video storage devices 532 can be used. Also alternatively or in combination with the foregoing, the microcontroller 510 can also perform the operations required to store and or retrieve video and other data in the video storage device 532.

[0057]   The video processing module 516 input can be directly supplied as a video output to a viewing device such as a video or computer monitor. In addition, the video and/or audio outputs can be supplied to an RF modulator 534 to produce an RF output and/or 8 vestigal side band (VSB) suitable as an input signal to a conventional television tuner. This allows the receiver 126 to operate with televisions without a video output.

[0058]   Each of the satellites 108 comprises a transponder, which accepts program information from the uplink center 104, and relays this information to the subscriber receiving station 110. Known multiplexing techniques are used so that multiple channels can be provided to the user. These multiplexing techniques include, by way of example, various statistical or other time domain multiplexing techniques and polarization multiplexing. In one embodiment of the invention, a single transponder operating at a single frequency band carries a plurality of channels identified by respective service channel identification (SCID).

[0059]   Preferably, the IRD 126 also receives and stores a program guide in a memory available to the microcontroller 510. Typically, the program guide is received in one or more data packets in the data stream from the satellite 108. The program guide can be accessed and searched by the execution of suitable operation steps implemented by the microcontroller 510 and stored in the processor ROM 538. The program guide may include data to map viewer channel numbers to satellite transponders and service channel identifications (SCIDs), and also provide TV program listing information to the subscriber 122 identifying program events.

[0060]   The functionality implemented in the IRD 126 depicted in FIG. 5 can be implemented by one or more hardware modules, one or more software modules defining instructions performed by a processor, or a combination of both.

Access Card

[0061] A CAM 512 often contains a microprocessor, memory components (a volatile component and a nonvolatile component) and a system input/output (I/O) module to communicate with transport 508. Traditional microprocessors within a CAM 512 have

5 nonvolatile memory to contain state that is used to provide the desired functionality and enforce security policies intended by the designers. The microprocessor and/or a memory access control unit restricts access to the memory components. Additionally, identification numbers may identify a CAM 512. However, in the prior art, there is no attempt to isolate the identification number from the system I/O module, system bus, microprocessor, or external

10 environment.

[0062] As described above, attacks may use unforeseen methods or may subvert poorly implemented defenses to gain unauthorized access to the contents of the memory and/or lead to reprogramming the contents of the memory. For example, most attacks occur by inappropriate manipulation of the microprocessor or memory access control unit. Reprogramming or

15 unauthorized access to the memory contents can lead to complete compromise of the security features intended in the CAM 512. The simplest and most prevalent form of attack against the memory component uses external means using the system I/O module due to the low cost of the equipment required to implement this form of attack. For example, the identification of the CAM 512 may be obtained through the system I/O module or microprocessor and duplicated

20 to create a pirate card.

[0063] The invention specifically attempts to secure memory content by hiding it from the external environment by ensuring that it is not placed on the system bus and not available to the microprocessor or system I/O module. Accordingly, to avoid the above-described methods of attack, access to the identification number is hidden by storing the number in a protected

25 nonvolatile memory component not directly connected to the system I/O module, system bus, or microprocessor. The custom logic block is implemented in solid state hardware that implements a simple and well defined state machine. The functions defined in the custom logic block specify a handful of well-defined operations that may be performed using the hidden identification

number. By preventing the system I/O module, system bus, microprocessor, or memory access control unit from direct access to the protected nonvolatile memory component (and thereby the identification number and identity of the CAM 512) the previously successful attacks are no longer possible.

5   [0064]   FIGS. 6A and 6B illustrate two architectures of a CAM 512 in accordance with one or more embodiments of the invention. The CAM 512 contains a microprocessor 602, volatile memory components 604 (e.g., random access memory [RAM]), one or more nonvolatile memory components 606 (e.g., electrical erasable programmable read only memory [EEPROM], erasable programmable read only memory [EPROM], or battery packed RAM),

10   a system input/output module 608, a custom logic block 612, and a hidden identification number 614 (that is stored within a separate nonvolatile memory component 606). The various components of CAM 512 may be communicatively coupled to a system bus 610.

[0065]   Ensuring that the identification number 614 is protected from modification retains the uniqueness of the device (i.e., CAM 512) that is important to many security models. The

15   hidden identification number 614 may be embedded into the CAM 512 after manufacturing.

[0066]   In FIG. 6A, the hidden identification number 614 is programmed by the microprocessor 602 (across the system bus 610) using a one time programmable memory protected by a hardware fuse 616 that isolates the identification number 614 (and nonvolatile memory component 606 containing the identification number 614) from the microprocessor 602

20   after the identification number 614 is written. In other words, after the hidden identification number 614 is written, the fuse 616 is blown.

[0067]   In FIG. 6B, the hidden identification number 614 is programmed by the custom logic block 612 using a onetime programmable memory/write once connection 616. Thus, after the custom logic block 612 writes the hidden identification number 614, the connection 616 no

25   longer exists (e.g., it is destroyed). As in FIG. 6A, the write once connection 616 of FIG. 6B may be a hardware fuse that is blown after the hidden number 614 is written.

[0068]   Accordingly, in both FIG. 6A and FIG. 6B, after the hidden identification number 614 is written, the identification number 614 is protected because it is not accessible by the

microprocessor 602 and hence cannot be altered by external means. Once isolated, the hidden

identification number 614 may only be read (and not modified) by custom logic block 612

through the read only connection 618. The custom logic block 612 is implemented in solid state

hardware that implements a simple and well defined state machine. The functions defined in the

5   custom logic block 612 specify a handful of well-defined operations that may be performed

using the hidden identification number 614.

[0069]   In addition to the above, the microprocessor's 602 nonvolatile memory component

606 and the nonvolatile memory component containing the hidden number 614 may use the

same physical and logical address ranges since they are controlled and programmed by separate

10   entities. Alternatively, the two memory components 606 (and component 606 containing hidden

number 614) may use separate address ranges as the system designer sees fit. This helps

obscure use of the memory containing the hidden number 614 by potential attackers making it

more difficult to determine the memory map and usage of code segments within the CAM 512.

[0070]   Additionally, the two nonvolatile memory components 606 may share programming

15   charge pumps and programming control. If the pumps and/or programming control are shared,

care should be taken to ensure that data and address lines of the nonvolatile memory component

606 containing the hidden number 614 are routed only to the custom logic block 612. This

saves chip area and reduces chip cost. Accordingly, the microprocessor 602 cannot provide

control information that may lead to a subsequent attack on the protected/dedicated memory

20   component 606 (i.e., the component containing the hidden number 614). Sharing the charge

pumps may be preferred to ease timing and high voltage requirements of the entire chip within

CAM 512.

[0071]   There are many advantages to utilizing a hidden identification number 614. For

example, the hidden identification number 614 can withstand substantial external attacks without

25   inappropriately modifying the contents of the nonvolatile memory component 606 containing the

identification number. Further, by preventing the system I/O module 608, system bus 610,

microprocessor 602, or memory access control unit from directly accessing the hidden

identification number 614 contained in an isolated nonvolatile memory component 606, traditionally successful security compromises are no longer possible.

[0072] Additionally, the integrity of information is significantly improved through isolation of its storage component from the system I/O module 608, system bus 610, and/or microprocessor

5   602. Protecting the integrity of the hidden number 614 is important because it prevents/limits low cost cloning attacks where the identity of a pirate card is copied to a new card. This attack is limited through the hidden identification number 614.

[0073] Since the hidden identification number 614 can only be read by a custom logic block 612 and cannot be reprogrammed by the microprocessor 602, the identity of the CAM 512

10   cannot be transferred to a second CAM 512, thereby preventing a successful, low cost, clone attack. Thus, the identity of the device (i.e., the CAM 512) is protected for use in operations with the CAM 512, IRD 126, and headend. For example, the CAM 512 provides non-modifiable uniqueness (i.e., stored in protected memory 614) that can be used to prevent cloning of the CAM 512 to obtain unauthorized access. Additionally, the CAM 512 may

15   provide an IRD 126 for non-modifiable pairing and blacklist, and may provide a headend that controls access rights and blacklist. A blacklist is utilized to prevent CAMs 512 with a particular identification to be used/cloned. With a blacklist, the headend may provide a list of blacklisted/unauthorized cards to an IRD 126. The IRD 126 then refuses to grant access rights if the CAM 512 being utilized is on the blacklist. Accordingly, uniquely identified CAMs 512

20   with a unique identification that is only accessible through a custom logic block 612 may be utilized to prevent unauthorized access and cloning.

[0074] Preventing low cost attacks forces attackers to use expensive invasive attacks that are not available to the vast majority of pirates. Inhibiting this simple form of attack prevents intruders from using attacks that require only a personal computer and a $10 card reader.

25   Instead, pirates are forced to utilize sophisticated, costly, and time consuming invasive attacks in which the actual hardware is modified. Additionally, further compromise of one device through an internal, invasive attack does not lead to a successful attack through a low cost, external attack.

[0075] FIG. 7 is a flow chart illustrating the use of hidden identification number 614 to limit unauthorized access to digital services in accordance with one or more embodiments of the invention. At step 700, the hidden non-modifiable identification number 614 is embedded (e.g., by a microprocessor 602 or a custom logic block 612) into a nonvolatile memory component

5   606. The number 614 uniquely identifies a device (e.g., CAM 512) that contains the nonvolatile memory component 606 (that contains the number 614). Such embedding occurs after manufacturing the CAM 512. As described above, the nonvolatile memory component 606 is used to contain state information to provide desired functionality and enforce one or more security policies for accessing digital services.

10   [0076] At step 702, access to the nonvolatile memory component 606 is isolated such that the identification number 614 (and nonvolatile memory component containing the hidden number 614) is protected from modification such that the nonvolatile memory component 606 is read only. The memory component 606 may be isolated by preventing a system I/O module 608, system bus 610, microprocessor 602, or external environment from direct access to the

15   identification number 614. For example, as described above, the identification number 614 may be embedded using a onetime programmable memory that is protected by a hardware fuse that isolates the identification number 614/and component 606 from the microprocessor 602 after the identification number 614 is written.

[0077] At step 704, the identification number 614 is read by a custom logic block 612. The

20   identification number 614 may be read for use in a function defined in the custom logic block 612, wherein the function specifies an operation to be performed using the identification number 614. For example, to activate or ensure that a user is authorized to receive/use broadcast digital services, the identification number 614 may be read by the custom logic block 612 pursuant to a security policy enforced by the nonvolatile memory 606 within CAM 512. Thus, access to the

25   digital services are based on access rights associated with the hidden non-modifiable identification number 614. For example, if the hidden number 614 exists on a blacklist (i.e., a list of unauthorized numbers 614 as described above), access to the digital services may be rejected.

[0078] Thus, as described, the identification number 614 is embedded into nonvolatile memory 606 (at step 700) and the nonvolatile memory 606 is isolated (thereby hiding access to and modification of the identification number 614) (at step 702). Once the identification number 614 has been embedded into the memory 606, the card maintains a non-modifiable identity that can then be used to enforce a security policy (e.g., by reading the identification 614 at step 704) based on that unique identity.

[0079] The use of an identification number 614 in this manner significantly improves the integrity of information through isolation of the information's storage component (e.g., nonvolatile memory 606) from the system I/O module 608, system bus 610, and/or microprocessor 602. Manipulation of stored content is also reduced through direct connection of a read-only fixed state custom logic block machine 612. Thus, information (e.g., the identification number 614 or other information) may be written once, and hidden from the system I/O module 608, system bus 610, and/or microprocessor 602. Further, the custom logic block 612 can be used to hide information from these other components.

Conclusion

[0080] This concludes the description of one or more embodiments of the present invention. The foregoing description of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. Accordingly, while the invention may protect video, audio, broadband and data services reception using a microcircuit that resides in a smart card and set top box, the invention is not limited to smart card applications or to a particular digital service system.

[0081] It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.